

REMARKS

The application has been amended and is believed to be in condition for allowance.

Certain of the previously pending claims have been amended and new claims are added. Claim 22 corresponds generally to claim 1. In general, the new dependent claims recited more specific combinations found in the independent claims.

Claims 1, 5 and 15-17 were objected to because of certain informalities set out in the Official Action. All the mentioned informalities have been corrected in the claims concerned as kindly suggested by the Examiner.

Claims 1, 5 and 15-17 are also rejected as being indefinite in the use of the term "signal pattern seen within the content of the transmission".

Claims 1, 5 and 15-17 have been amended and in the amended claims the term referred to has been replaced by "the transmission content patterns within the packets of the transmission".

The term "the transmission content patterns within the packets of the transmission" is believed to be clear. Information transmitted in a communications network such as the Internet is transmitted in packets. Content patterns in the packets vary according to the types of or combination of types of information. For example, a packet containing image information has different transmission content patterns to those in a packet containing

only text information. Content patterns for words of the same meanings in different languages are considerably different from each other. Through analyzing transmission content patterns in packets, words in any language can be predicted. This is different to counting words which are in ASCII codes of 1s and 0s.

Claims 1, 5 and 7-13 stand rejected as anticipated by RUSSELL-FALLA et al. 6,266,664.

Claim 14 stands rejected as being unpatentable over RUSSELL-FALLA in view of BAKER et al. 5,678,041.

Claims 15-17 stand rejected as being unpatentable over RUSSELL-FALLA in view of INAKOSHI 5,933,604.

#### The Prior Art

RUSSELL-FALLA teaches a process for blocking a display of a web page that contains a particular type of content. The process is incorporated into a blocking computer program installed on a user computer and operates in conjunction with a web browser client program running on the user computer. The blocking computer program configures the user computer as a proxy server (10) which intercepts web pages downloaded to the user computer following requests (50) made with the browser program on the user computer. The downloaded web pages are cached either in a hard disk or a random access memory (RAM) unit of the user computer and the cached web pages are analyzed for determining

whether they can or cannot be displayed on a display screen (52) of the user computer.

The analysis involves a first step (14) of scanning each cached web page (12) to identify regular text expressions in the web page. For each text expression the blocking computer program queries a pre-existing database (30) containing previously input text expressions that relate to the particular type of content to be blocked from viewing to determine whether or not the expression appears in the database. Where the expression being queried matches one in the database, the matched expression is entered into a "match list" (20). The expressions in the database are individually weighted and the blocking program is arranged to lookup the weighting corresponding to each matched expression to form a weighted list (42) of matching expressions. A rating value (46) of the matching expressions is then calculated based on dividing a scaled summation of the weightings in the weighted list with the total number of words in the initial expressions for analysis.

The blocking software uses a neural network architecture to develop text expressions for the database and their weighs. The neural network (72) applies a random weighting to each regular expression of words extracted from a large number of training data (70) such as a collection of web pages, to form a weighted list (78) of regular text expressions. The weightings for the expressions are repeatedly adjusted by comparing with

predetermined "good" and "bad" web pages to arrive at a set of weightings that are considered to be predictive of the selected type of content.

The blocking program allows a user nominated as the administrator to configure it to block web pages having specified types of content for individual users of the user computer and to allocate a rating value for a particular type of content for each user. Where a rating value is calculated for a downloaded web page, the blocking program compares the calculated rating value of the downloaded web page at step (60) with predetermined threshold values allocated for individual users in step (56) to determine whether or not the downloaded page is to be display on the display (52) by controlling a gate (64). A default rating value is used for any user without an allocated rating value. If the calculated rating value of the web page exceeds the applicable allocated threshold value for the particular user, the gate (64) is controlled by a control signal (62) to prevent the web page from being displayed at the browser display (52). The administrator can however review the blocked web page and overrule the blocking program by adding the URL of the web site sending the web page to a "do not block" list of web sites.

The blocking program taught in RUSSELL-FALLA is similar to the prior art mentioned from specification page 1, line 26 to page 2, line 1.

Such prior art blocking program is installed on a user computer and therefore it can be easily removed, disabled or otherwise circumvented by adding URLs of undesirable web pages to the "do not block" list or posing as the administrator to view any downloaded web pages. The blocking program determines whether a downloaded web page can or cannot be viewed by a user on the basis of a comparison of a calculated rating value of discernible regular expressions of words or phrases in the web page with a threshold value allocated to a user. This program will not block undesirable graphic images on web pages which either do not have words or have words deemed to be good.

The Amended/New Claims

In view of comments in the Official Action, the applicant has substantially revised independent claims 1 and 5 so that the apparatus in the amended claims is clearly distinguished from the blocking program taught in RUSSELL-FALLA.

The prior art does not teach or suggest any of: (1) capturing the packets of information before reaching a remote requesting communications terminal; (2) using a statistical modelling arrangement for predicting the content category of the captured packets based on a comparison of the transmission interaction characteristics in the captured packets with the transmission interaction characteristics of packets of information of a known content category to predict the content category; and (3) preventing the captured packets belonging to

information predicted to be of an undesirable category from reaching the remote communications terminal.

Amended claims 1 and 5 recite an apparatus for classifying information having at least one image transmitted over a communications network into content category classifications.

The apparatus comprises a first means arranged to capture network packets or fragments of the packets in a session of transmission of the information from an information providing communications terminal on a path of the communications network. As each packet contains the IP address of the communications terminal providing the information, the apparatus of this invention can determine from the captured packets whether the information is or is not from a known source by comparing the IP addresses with those in a database of content servers deemed to be undesirable. Those packets from content servers deemed to be undesirable are not forwarded to the user communications terminals requesting the information.

The first means is also adapted to obtain one or more transmission interaction characteristics based on content of the captured packets.

The apparatus also has a second analyzing means having a statistical model arranged for predicting a content category classification of unknown captured information based on statistical modeling analysis of said one or more transmission

interaction characteristics obtained from the captured packets with those of known information without input or relevancy as to a particular user. The one or more transmission interaction characteristics include any one or more of: date and time stamps of the captured packets, size of image transmission activities, size of text transmission activities, ratio of image to text transmission activities, and variations in content patterns of the text and image within the captured packets.

The apparatus of the invention responds to the predicted content category classification to determine whether the captured packets of the information are or are not to be released for forwarding to the remote user communications terminal. The captured packets are released for forwarding to the remote user terminal only if the predicted content category of the captured packets by the statistic modeling is not amongst a list of known undesirable content classifications.

As information deemed to be undesirable does not reach the user terminals, it is not possible to view the undesirable information on the user terminals. Moreover, as the apparatus as recited in claims 1 and 5 captures all communications traffic upstream of user terminals, one apparatus can serve a large number of user terminals connecting through a common gateway, such as an Internet Service Provider, There is no need to have a blocking control program installed on each user terminal.

The blocking program taught in the RUSSELL-FALLA predicts ratings of information based on text expressions in information downloaded in a user computer. As such, the blocking computer must be installed on each user computer and the user computers must each be trained to block particular content types based on text expressions. The instant invention, however, predicts content type classifications of information transmitted over a communications network by statistic modeling of certain transmission interaction characteristics of the captured packets, and the transmitted information does not reach the intended user computer if it is predicted to be of an undesirable content category.

More importantly, the blocking program taught in RUSSELL-FALLA is limited to block only text based information. RUSSELL-FALLA does not teach an apparatus for blocking information in the form of undesirable images as claimed in the instant invention.

The applicant therefore believes amended claims 1 and 5 are not anticipated by RUSSELL-FALLA. As all other claims are dependent from either claim 1 or claim 5, these claims are accordingly also not anticipated.

These comments also apply to the new claims.

In the Official Action, the collection of training pages described in the RUSSELL-FALLA patent appears to be interpreted as a form of the profiling means claimed in claims 10



to 13. The applicant respectfully disagrees with such interpretation. The blocking program taught in the RUSSELL-FALLA patent simply designates the training pages as either "good" or "bad" based on the text expressions on those pages, and the training pages are used to determine appropriate weightings of the text expressions. The RUSSELL-FALLA patent does not teach nor hint at analyzing transmission interaction characteristics in captured network packets to profile user terminals and content servers.

The BAKER et al. patent teaches a system for selectively restricting access to one or more uniform resource locators (URLs) which may be content servers. The system of the BAKER et al. patent has a proxy server (112) configured to control access level of individual user terminals (107, 108 and 109) in a local area network (110) to URLs (101, 102, 103, 104 and 105) via a public network (100). For controlling the access levels, the proxy server (112) has a database (114) with a listing (115) of user terminal clearances for each user terminal, and a listing (116) of URL ratings based on NV for non violent, MV for moderately violent, and V for violent. When a requesting user terminal transmit a URL via LAN (110), a processor (111) in the proxy server (112) queries the listing (115) to determine the allowable resource ratings for the particular requesting terminal, and the listing (116) to determine the resource rating of the URL for accessing. If the rating of the URL for accessing

is not amongst the clearances set for the requesting terminal, the processor (111) denies the request and the requested URL is not sent to the public network (100). Conversely, if the user terminal has clearance for the URL rating, the processor (111) forwards the requested URL. All the URL ratings and the clearances for the user terminals are subjectively categorized by a system administrator.

The system of the BAKER et al. patent does not analyze information downloaded to a user terminal for determining whether the downloaded information can or cannot be displayed on the display unit of the user terminal. Instead, it prevents a URL request from a user terminal from being forwarded to a public network such as the Internet, if a system administrator has categorized this URL with a level which the user terminal has not been cleared by the system administrator to access. Accordingly, the BAKER et al. patent teaches away the apparatus of the RUSSELL-FALLA patent.

Moreover, the BAKER et al. patent does not teach capturing of network packets of information containing at least one image from a content server and obtaining transmission interaction characteristics of the captured packets. BAKER et al. also does not teach the application of a statistic model to the obtained transmission interaction characteristics of the packets from an unknown content server for determining whether the packets are or are not to be forwarded to a requesting user

terminal. Thus, modifying the apparatus in the RUSSELL-FALLA patent to selectively control network access of the user terminals as taught by the BAKER et al. patent would not result in the apparatus as claimed in the present application. The applicant therefore believes the apparatus as claimed in claim 14 is not obvious in view of the RUSSELL-FALLA patent and the BAKER et al. patent.

The INAKOSHI patent teaches a network resource monitoring system for informing users of a change in any web page on a destination web site URL for which monitoring has been requested. As described with reference to Figure 8, the system of INAKOSHI has a management unit (12) which receives monitoring requests from users using an input interface (10) such as a browser software or an email application. Each of the requests includes the URL of the when page for monitoring, and the URL for reporting to the requesting user. The management unit delegates a number of delegate places (51) of a monitoring arrangement (13) to periodically access web pages having an address in a local area in order to minimize communications costs. When accessing a web page, the delegate place checks the file size of the web page and informs the management unit of the time of access and the file size. The management unit then informs the users who requested monitoring of any change in the file size of the web pages.

The INAKOSHI system merely informs users of any updates for the web pages of interest to the requesting users. The web pages are not downloaded to the requesting user terminals and are not analyzed to determine their content. As there are no transmission of the contents of the web pages, there can be no transmission interaction characteristics. Accordingly, there is no incentive to incorporate the INAKOSHI system into the RUSSELL-FALLA apparatus.

Moreover, the INAKOSHI patent does not teach capturing of network packets of information containing at least one image from a content server and obtaining transmission interaction characteristics of the captured packets. INAKOSHI also does not teach the application of a statistic model to the obtained transmission interaction characteristics of the packets from an unknown content server for determining whether the packets are or are not to be forwarded to a requesting user terminal. Thus, modifying the apparatus in the RUSSELL-FALLA patent to monitor any update of web pages as taught by the INAKOSHI patent would not result in the apparatus as claimed in the present application. The applicant therefore believes the apparatus as claimed in claims 15 to 17 is not obvious in view of the RUSSELL-FALLA patent and the INAKOSHI patent.


In light of the above remarks, the applicant respectfully submits the claims as presented are both novel and are non-obvious.

Therefore, reconsideration and allowance of all the claims are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949  
745 South 23<sup>rd</sup> Street  
Arlington, VA 22202  
Telephone (703) 521-2297  
Telefax (703) 685-0573  
(703) 979-4709

REL/mjr